حاجی زین‌العابدینی، محسن؛ رفعتی، مینا (۱۳۹۶). بررسی نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران. *پژوهش‌های نظری و کاربردی در علم اطلاعات و دانش‌شناسی*، ۷ (۱)، ۲۵۷- ۲۷۹.

بررسی نظام مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران

محسن حاجی زین العابدینی، استادیار گروه علم اطلاعات و دانش‌شناسی دانشگاه شهید بهشتی، zabedini@gmail.com
مینا رفعتی، کارشناس ارشد علم اطلاعات و دانش‌شناسی، rafati7339@yahoo.com

تاریخ دریافت: ۹۵/۱/۲۹ تاریخ پذیرش: ۹۵/۸/۲۵

دوفصلنامه| (علمی پژوهشی)
پژوهش‌های نظری و کاربردی در علم اطلاعات و دانش شناسی

شاپا (آنلاین): ۲۵۳۸-۴۱۱۲

http://infosci.um.ac.ir

سال ۷ (شماره ۱)
بهار و تابستان ۱۳۹۶

DOI: 10.22067/55215

چکیده:

مقدمه: *هدف این پژوهش شناسایی نظام مدیریت امنیت اطلاعات (امنیت فیزیکی، امنیت ارتباطات، کنترل دسترسی به اطلاعات، مدیریت حوادث امنیت اطلاعات و مدیریت پیوستگی عملیات) در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران است. ضرورت انجام این پژوهش از آنجا احساس می‌شود که در رشته علوم کتابداری و اطلاع‌رسانی به امر حفاظت و امنیت کتابخانه‌ها کم‌تر توجه شده است.*

روش‌شناسی: *روش پژوهش پیمایشی تحلیلی است. جامعه آماری این پژوهش کلیه مدیران کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران است که در سال ۱۳۹۱، ۲۵ مدیر بوده‌اند. پرسش های پژوهش عبارتست از: تا چه میزان امنیت فیزیکی در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران رعایت می‌شود؟ تا چه میزان از امنیت و عملکرد صحیح تجهیزات (نظیر رایانه‌ها) و پردازش اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران اطمینان حاصل می‌شود؟ تا چه میزان جهت دسترسی به اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران کنترل صورت می‌گیرد؟ تا چه میزان در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران در صورت وقوع حادثه در کتابخانه، راهکارهای مدیریتی مرتبط با امنیت کتابخانه رعایت می‌شود؟ تا چه میزان از استمرار در فعالیت‌ها (عدم وقفه در فعالیت‌ها) در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران اطمینان حاصل می‌شود؟ در پژوهش حاضر برای گردآوری اطلاعات از پرسشنامه محقق ساخته بهره گرفته شده است. جهت*

تجزیه‌وتحلیل داده‌ها از آمار توصیفی همچون فراوانی و درصد، آزمون t تک متغیری و آزمون مجذور کا یا خی استفاده شد. برای مقایسه مؤلفه‌های مدیریت امنیت اطلاعات از نظر میزان رعایت آنها آزمون فریدمن به‌کار گرفته شده است.

یافته‌ها: *همان‌طور که یافته‌ها نشان می‌دهد مؤلفه‌های مطرح شده تا حد زیادی در کتابخانه‌های مرکزی رعایت می‌شود. چنانچه هر یک از مدیران، کارمندان و کاربران کتابخانه‌ها دستورالعمل‌های مرتبط با مؤلفه‌های امنیت اطلاعات را به طریق صحیح رعایت نمایند می‌توان امیدوار بود امنیت اطلاعات در کتابخانه‌های مورد بررسی به‌طور نسبی رعایت شود.*

بحث و نتیجه‌گیری: *نتایج نشان می‌دهد مؤلفه‌ها تا حد زیادی در کتابخانه‌های مرکزی رعایت می‌شود. لازم است جهت امنیت فیزیکی وسایل شخصی افراد تحویل گرفته شود، درگاه‌های حفاظتی، دوربین مداربسته و ... لحاظ گردد. جهت امنیت ارتباطات از نظام‌های اطلاعاتی‌ای در کتابخانه‌ها استفاده شود که: به‌روز باشند، به لحاظ امنیتی پشتیبانی شوند، بتوانند تحت وب باشند. جهت امنیت کنترل دسترسی سطوح دسترسی افراد به منابع کتابخانه‌ای را مشخص نمایند. همچنین، موارد امنیتی جهت جلوگیری از آتش‌سوزی، قطعی برق، زلزله، سیل و ... لحاظ گردد. جهت مدیریت پیوستگی عملیات، فرآیندهای کتابخانه‌ای در فواصل منظم و نامنظم مورد بررسی قرار گیرند.*

کلیدواژه‌ها: *امنیت اطلاعات، استاندارد ISO27001، امنیت فیزیکی، امنیت ارتباطات، کنترل دسترسی، مدیریت حوادث، مدیریت پیوستگی عملیات.*

مقدمه

اطلاعات در سازمان‌ها، مؤسسات پیشرفته و جوامع علمی شاهرگ حیاتی محسوب می‌گردد. دستیابی به اطلاعات و ارائه مناسب و سریع آن همواره مورد توجه سازمان‌هایی است که اطلاعات در آنها دارای نقش محوری و سرنوشت‌ساز است.

سرعت در تولید و عرضه اطلاعات ارزشمند یکی از رموز موفقیت در سازمان‌ها، مؤسسات و جوامع علمی در عصر اطلاعات است. پس از سازماندهی اطلاعات باید با بهره‌گیری از شبکه‌های رایانه‌ای زمینه استفاده قانونمند و هدفمند از اطلاعات را برای دیگران فراهم کرد. به موازات حرکت به‌سمت یک سازمان پیشرفته و مبتنی بر فناوری اطلاعات باید تدابیر لازم در رابطه با حفاظت از اطلاعات نیز اندیشیده شود (اسدی، ۱۳۸۴). به‌عبارت دیگر نیاز روزافزون به استفاده از فناوری‌های نوین در ارائه اطلاعات و ارتباطات، ضرورت استقرار یک نظام مدیریت امنیت اطلاعات را بیش‌ازپیش آشکار می‌نماید. از این‌رو حفظ ایمنی فضای تبادل اطلاعات از جمله مهمترین اهداف توسعه فناوری اطلاعاتی و ارتباطی محسوب می‌شود . بدیهی است که توجه نکردن به تأمین امنیت فضای تبادل اطلاعات و برخورد نادرست با این مقوله مانع از گسترش فضای مذکور در میان آحاد جامعه و جلب اعتماد مدیران در به‌کارگیری روش‌های نوین نظارتی و اطلاع‌رسانی خواهد شد (پورمند، ۱۳۸۵).

در حال حاضر، وضعیت امنیت فضای تبادل اطلاعات کشور، به‌ویژه در مؤسسه‌ها و سازمان‌های

دولتی و خصوصی، در سطح مطلوبی قرار ندارد. از جمله دلایل اصلی وضعیت موجود، می‌توان به فقدان زیرساخت‌های فنی و اجرایی امنیت و عدم انجام اقدام‌های مؤثر در خصوص ایمن‌سازی فضای تبادل اطلاعات مؤسسه‌ها و سازمان‌ها اشاره نمود (داوری دولت‌آبادی، ۱۳۸۹).

در کتابخانه‌ها منابع اطلاعاتی با هزینه‌های بسیار زیادی تهیه و برای استفاده مهیا می‌شوند. هزینه‌های تهیه و نگه‌داری منابع و اطلاعات و امنیت آنها یک وجه مسئله است و دسترسی و مهیاسازی آنها برای استفاده، وجه دیگر ارائه خدمات در کتابخانه‌ها و مراکز اطلاع‌رسانی است. منابع گردآوری شده در کتابخانه‌ها به‌منظور استفاده همگانی تهیه و تدارک دیده شده‌اند نه برای استفاده یک قشر خاص. بنابراین خارج شدن غیرقانونی یک منبع از کتابخانه به‌معنای عدم دسترسی استفاده‌کنندگان کتابخانه به آن منبع برای همیشه است. این مسئله در مورد نسخ نایاب و کم‌یاب صدمات بیشتری را در پی دارد. چون دیگر نمی‌توان جایگزینی برای این منابع پیدا کرد. اقداماتی که برای جلوگیری از دزدی، بریدن و ناقص کردن کتاب‌ها انجام می‌گیرد، بخش مهمی از فعالیت‌های امنیتی را در اغلب کتابخانه‌ها شامل می‌شود. اغلب کتابخانه‌ها علاوه بر اینکه باید هزینه‌های کتاب‌های دزدیده و پاره شده را تأمین نمایند، به دشواری خواهند توانست ناراحتی و عصبانیتی را که این مشکلات در خوانندگان به‌وجود می‌آورد، برطرف سازند (هاروی، ۱۳۸۴).

در عصر فناوری اطلاعات در کنار تسهیل فرآیندهای کاری کتابخانه‌ها بحث مدیریت امنیت اطلاعات اهمیت بیشتری دارد. عدم توجه برخی کاربران کتابخانه‌ها که با صدمات فیزیکی به منابع چاپی و غیرچاپی باعث تخریب و نابودی اطلاعات می‌شوند، همچنین کتابخانه‌ها به‌علت رعایت نکردن امنیت ارتباطات با فقدان زیرساخت‌های فنی و اجرایی و عدم انجام اقدامات مؤثر در خصوص ایمن‌سازی روبرو هستند و نیز بازرسی کافی از تجهیزات و سامانه‌ها نمی‌شود. بنابراین برخی از چالش‌هایی که ضرورت پرداختن به مسائل امنیتی در کتابخانه‌ها را توجیه می‌کند، بیان شد که عبارتند از: سرقت منابع اطلاعاتی و تجهیزات کتابخانه، صدمه‌زدن و تخریب منابع کتابخانه، عدم عکس‌العمل سریع فعالیت‌های کتابخانه در صورت وقوع حوادث امنیتی (نظیر سیل، زلزله، آتش‌سوزی، ترکیدگی لوله و ...)، عدم استفاده از نظام‌های امنیتی پیشرفته و مسائل دیگر.

اگر به نظام مدیریت امنیت اطلاعات به‌صورت کلان نگریسته شود شامل: امنیت فیزیکی، امنیت کارمندان، امنیت ارتباطات، کنترل دسترسی به اطلاعات، مدیریت حوادث امنیت اطلاعات، مدیریت پیوستگی عملیات و ... است.

ضرورت انجام این پژوهش از آنجا احساس می‌شود که در رشته علوم کتابداری و اطلاع‌رسانی به امر حفاظت و امنیت کتابخانه‌ها کم‌تر توجه شده است، از جمله در سازمان‌ها و استانداردهای زیر مانند:

ساختمان و تجهیزات کتابخانه، استاندارد کتابخانه‌های دانشگاهی، استاندارد کتابخانه‌های تخصصی، حفاظت و نگه‌داری مواد کتابخانه. در هیچ‌یک از حوزه‌های مذکور به ایمنی و حفاظت از کتابخانه در برابر رعایت مقررات امانت، انواع دستبردها در ساعات تعطیلی کتابخانه و مدیریت ایمنی کتابخانه به‌صورت عملی و کاربردی و براساس استانداردهای موجود پرداخته نشده است. لذا تحقیقات در این زمینه کاملاً ضروری به‌نظر می‌رسد زیرا در قالب آن می‌توان با حفاظت و امنیت از اطلاعات کتابخانه براساس استانداردهای موجود بین‌المللی آشنا گردیده و از آنها بهره‌مند شد.

امنیت[۱]

امنیت معمولاً به نظام یا فعالیتی اطلاق می‌گردد که برای جلوگیری از سرقت و دانش‌ستیزی به‌کار مانند نظام کنترل کتابخانه، نظام امنیتی کتاب، حفاظ‌های امنیت و نظایر آنها می‌رود. امنیت همچنین فرآیندی است که حفاظت از مجموعه‌ها، ابزار، اطلاعات، کارمندان و تسهیلات فیزیکی را فراهم می‌کند و از تأثیرات نامطلوب، غیرمجاز و زیان‌آور به اهداف کتابخانه‌ها و آرشیوها جلوگیری می‌نماید. به زبان ساده‌تر فعالیت‌هایی که یک مؤسسه یا سازمان برای محافظت از مراجعان، کارکنان و مجموعه‌هایش از آسیب‌ها انجام می‌دهد (جوکار، ۱۳۸۳).

امنیت اطلاعات[۲]

امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن دسترسی غیرمجاز به آنها اشاره می‌کند (جعفری، صادقی‌مجرد، ۱۳۸۶).

امنیت اطلاعات اصولاً در رعایت سه خصیصه زیر تأمین می‌شود:

۱. محرمانه بودن اطلاعات[۳]: اطمینان از اینکه اطلاعات می‌توانند تنها در دسترس کسانی باشند که مجوز دارند.

۲. صحت اطلاعات[۴]: حفاظت از دقت و صحت اطلاعات و راه‌های مناسب پردازش آن اطلاعات

---

1. Security
2. Information Security
3. Confidentiality of information
4. Accuracy of information

۳. در دسترس بودن اطلاعات[1]: اطمینان از اینکه کاربران مجاز در هر زمان که نیاز داشته باشند، امکان دسترسی به اطلاعات وجود داشته باشد (پورمند، ۱۳۸۵).

مدیریت امنیت اطلاعات[2]

بر طبق چهارچوب امنیت اطلاعات، مدیریت امنیت اطلاعات به‌معنی حفاظت سازمان از ریسک‌های شناخته شده با نظام‌های اطلاعات تحت کنترل درون سازمانی و ایجاد یک محیط امن می‌باشد (Swanson, 2006).

مدیریت امنیت اطلاعات وظیفه تعیین اهداف امنیت و بررسی موانع سر راه رسیدن به این اهداف و ارائه راهکارهای لازم را برعهده دارد. هم‌چنین مدیریت وظیفه پیاده‌سازی و کنترل عملکرد نظام امنیت سازمان را برعهده داشته و در نهایت باید تلاش کند تا نظام را همیشه روزآمد نگه دارد (امیرخانی و توکلی، ۱۳۸۸).

نظام مدیریت امنیت اطلاعات[3]

نظام مدیریت امنیت اطلاعات بخشی از سیستم مدیریت کلی و سراسری در یک سازمان است که بر پایه رویکرد مخاطرات کسب و کار قرار داشته و هدف آن پایه‌گذاری، پیاده‌سازی، بهره‌برداری، نظارت، بازبینی، نگه‌داری و بهبود امنیت اطلاعات است (سیفی و شربت‌اوغلی، ۱۳۸۶).

استاندارد نظام مدیریت امنیت اطلاعات (ISO 27001)[4]

استاندارد ISO 27001 یکی از رایج‌ترین و شناخته شده‌ترین استانداردها برای نظام‌های مدیریت امنیت اطلاعات بوده و برای هر سازمانی در هر بخش قابل اجرا می‌باشد. این استاندارد رویکردی جامع در حفاظت از اطلاعاتی که نیاز به حفاظت دارند شامل دامنه‌ای از اطلاعات دیجیتال، مستندات کاغذی و ... تا دانش فردی کارمندان را عرضه می‌نمایند. استاندارد ISO27001 دارای ۱۱ بخش اصلی است که در مدیریت امنیت اطلاعات نیز به‌کار گرفته شده‌اند (داوری دولت‌آبادی، خراسانی راد، حسین‌آبادی و امیرزاده، ۱۳۸۹).

سازمان‌ها و نظام‌های اطلاعاتی و شبکه‌های ارتباطی آنان به‌طور روزافزون در معرض تهدیدهای امنیتی گسترده‌ای از قبیل کلاهبرداری به کمک رایانه، جاسوسی، آتش‌سوزی و سیل هستند (سیفی و

1. Availability of information
2. Information Security Management
3. Information Security Management System
4. International Organization for Standardization 27001

شربت‌اوغلی، ۱۳۸۶). لازم است تمامی افراد سازمان به حداقل استانداردها در مورد رعایت نکات امنیتی واقف باشند و به آن عمل کنند (معتمدی‌فر، ۱۳۸۷).

هدف این استاندارد کمک به سازمان‌هایی است که نظام مدیریت امنیت اطلاعات را ایجاد نموده و سپس نگه‌داری می‌نمایند. ما در این مجال به‌دلیل اهمیت امنیت فیزیکی در منابع اطلاعاتی کتابخانه، امنیت ارتباطات در نرم‌افزارها و شبکه‌های کتابخانه‌ای، کنترل دسترسی به‌جهت متفاوت بودن سطح دسترسی کاربران، کارکنان و مدیران، مدیریت حوادث در جهت پیش‌بینی‌های لازم برای حوادثی نظیر سیل، آتش‌سوزی و ... و مدیریت پیوستگی عملیات به‌جهت بازنگری دستورالعمل‌های امنیتی کتابخانه از نظام مدیریت امنیت اطلاعات می‌پردازیم.

امنیت فیزیکی[۱]

حفاظت فیزیکی اصلی مهم در رعایت ایجاد امنیت می‌باشد که از طریق ایجاد موانع چندگانه فیزیکی در اطراف منابع سازمانی و تجهیزات پردازش اطلاعات امکان‌پذیر است. هر یک از مرزهای ایجاد شده، دسته‌ای از منابع سازمانی را در برگرفته و افزایش این منابع، سطح کلی حفاظت را افزایش می‌دهد. باید با استفاده از این موانع امنیتی، تجهیزات پردازش اطلاعات را حفاظت نمود.

لازم است تجهیزات حساس و اطلاعات سازمان در مکانی امن که براساس تعاریف امنیتی از پیش تعیین شده، نگه‌داری کرد. این مکان باید دارای مرزهای امنیتی بوده و ورود و خروج از آن کنترل شود هدف از تدوین امنیت فیزیکی موارد زیر می‌باشد:

- جلوگیری از دستیابی غیرمجاز، وارد کردن صدمه و تداخل به اطلاعات سازمان در محیط‌های امن؛
- جلوگیری از تلف‌شدن و واردآمدن صدمه به دارایی‌ها و وقفه در کار تجهیزات سازمان؛
- جلوگیری از دزدی اطلاعات و فن‌آوری‌های اطلاعات (ایزو/آی ای سی ۲۷۰۰۱: ۲۰۰۵، ۱۳۸۹).

مدیریت ارتباطات[۲]

با ورود به دنیای اینترنت و استفاده روزافزون کتابخانه‌ها از شبکه‌های رایانه‌ای، منابع پیوسته و دیجیتالی نظام‌های خودکار، مسئله تأمین امنیت شبکه‌های کتابخانه‌ای به‌وجود آمده است (جوکار، ۱۳۸۳). ایجاد شبکه‌ای امن از رایانه‌های کتابخانه بیشتر از هر زمان دیگری مهم‌تر است. هم‌زمان که مدیر شبکه از

1. Physical Security
2. Communications Management

نظام‌ها و رایانه‌های کتابخانه محافظت می‌کند، دسترسی عمومی به رایانه‌ها برای دسترسی به اطلاعات مورد نیاز را تضمین می‌نماید. همچنین از طریق دسترسی قانونی امکان اشتراک با منابع را مهیا می‌سازد. در کتابخانه‌های بزرگتر برای اطمینان از امنیت نظامها و شبکه‌های کتابخانه علاوه بر مدیر شبکه به همکاری مهندسیار رایانه‌ای، کتابداران و کارمندان نیاز می‌باشد (Ayre, 2003).

این مدیریت بیانگر کنترلی است که یک سازمان را قادر می‌سازد تا ارتباط درست و امنی را بر روی دارایی‌های خود اعمال نماید. لازم است اطلاعات اصلی و نرم‌افزارهای اجرایی به‌صورت منظم و دوره‌ای کپی‌برداری شده و نسخه پشتیبان کامل نظام اطلاعاتی تکمیل گردد. همچنین باید تهیه نسخه پشتیبان به‌صورتی انجام پذیرد که بتوان بلافاصله بعد از وقوع یک حمله ضد امنیتی و یا خرابی تجهیزات نگه‌داری اطلاعات، به‌سرعت سیستم را احیا نموده و تداوم عملیات را امکان‌پذیر ساخت. در واقع هدف، حصول اطمینان از کارکرد صحیح و امن پردازش اطلاعات و هم‌چنین به‌حداقل رساندن مخاطرات ناشی از آزمایش نظام‌ها و حفظ یکپارچگی نرم‌افزار و اطلاعات است (ایزو/آی ای سی ۲۷۰۰۱: ۲۰۰۵، ۱۳۸۹).

کنترل دسترسی[1]

کنترل دسترسی به مجموعه سیاست‌ها و اقدامات مربوط به دادن اجازه یا ندادن اجازه برای دسترسی کاربر خاصی به منابع، یا محدود کردن دسترسی به منابع نظام‌های اطلاعاتی برای کاربران، برنامه‌ها یا دیگر نظام‌های مجاز اطلاق می‌شود (اسدی، ۱۳۸۴). کنترل دسترسی به اطلاعات در کتابخانه باید در چهارچوب محرمانگی، جامعیت و دسترس‌پذیری برای استفاده کاربران و کارمندان صورت پذیرد و از دسترسی کاربران و کارمندان کتابخانه و از عدم دسترسی افراد خطاکار اطمینان حاصل گردد. دسترسی به فناوری الکترونیکی، بهترین سیستم برای کنترل دسترسی به ساختمان کتابخانه و امکانات آن است (National Institute of Standard and Technology, 2006).

لازم است دسترسی به اطلاعات و پردازش‌های سازمان براساس نیازهای سازمانی و امنیتی کنترل گردد. این قاعده را باید در سیاست‌گذاری روش‌های انتشار اطلاعات و مجوزدهی رعایت نمود. لازم است قواعد دسترسی و حقوق هر یک از کاربران باید به‌دقت و صراحت بیان نمود. بایستی کاربران و ارائه‌دهندگان سرویس به نظام (کارمندان)، به‌روشنی در جریان نیازها و روش‌های کنترل دسترسی قرار گیرند.

لازم است یک رمز عبور در جهت سهولت کنترل دسترسی برای کارمندان و کاربران از طریق

---
1. Access Control

یک فرآیند مدیریتی رسمی اختصاص داده شود. تمامی کاربران و کارمندان باید یک شناسه کاربری برای استفاده شخصی خودشان داشته باشند. به‌عبارت دیگر در دسترس بودن تضمین می‌کند که کاربران مجاز یک نظام، به هنگام و بدون هیچ وقفه‌ای به اطلاعات موجود در سیستم دسترسی پیدا کنند. هدف کنترل دسترسی، کاربر پذیری و ایجاد قابلیت اعتماد و اطمینان کاربر است (ایزو/آی ای سی ۲۷۰۰۱: ۲۰۰۵، ۱۳۸۹).

مدیریت حوادث امنیت اطلاعات[1]

مدیر باید اقدامات مناسب برای جلوگیری از زیان‌هایی مثل خرابکاری، سرقت از مواد کتابخانه و ... را پیش‌بینی نماید و اقدامات مناسب برای کاهش تلفات فاجعه‌بار همچون سیل، زلزله، آتش‌سوزی و ... را پیش‌بینی کرده و راهبرد لازم در جهت کاهش میزان تلفات در صورت بروز حادثه را برنامه‌ریزی نماید و از میزان حادثه و تلفات گزارش تهیه نماید تا پیش‌بینی و پیشگیری را آسان‌تر نماید (Chair & et al, 2010).

رویدادهای امنیت اطلاعات باید در کوتاه‌ترین زمان ممکن از طریق مجاری مدیریتی مناسب گزارش شوند. تمامی کارکنان باید نسبت به یادداشت و گزارش‌دهی هر ضعف امنیتی مشاهده شده یا مورد سوءظن در نظام‌ها یا خدمات ملزم شوند.

به‌منظور حصول اطمینان از پاسخی سریع، مؤثر و منظم به حوادث امنیت اطلاعات، مسئولیت‌های مدیریتی و روش‌های اجرایی باید ایجاد شوند و برای اینکه نوع، حجم و هزینه‌های حوادث امنیتی، قابل اندازه‌گیری و پایش باشند باید سازوکارهای لازم ایجاد شوند و در صورت ایجاد حادثه بعد از آن، باید وارد اقدامات قانونی گردید و شواهد گردآوری، نگه‌داری و ارائه شوند (ایزو/آی ای سی ۲۷۰۰۱: ۲۰۰۵، ۱۳۸۹).

مدیریت پیوستگی عملیات[2]

هیچ استراتژی کامل نخواهد بود مگر آنکه به‌طور متناوب و در مقاطع زمانی برنامه‌ریزی شده مورد بازبینی و ارزیابی قرار بگیرد. گاهی در ارزیابی استراتژی امنیتی، به مواردی از تغییر، تکمیل یا اقدامات جدید نیاز خواهد بود. بدیهی است که با گذشت زمان شرایط تغییر خواهد کرد (معتمدی فر، ۱۳۸۷). مدیر

1. Information Security Incident Management
2. Business Continuity Management

باید به‌طور مستمر، راهبرد امنیت را مورد بازبینی و نقد قرار بدهد و نیازهای جدید را در آن لحاظ کند. لازم است با استفاده از ساز و کارهای پیشگیری و احیا مجدد، یک فرآیند مدیریت پیوستگی عملیات سازمانی طراحی شود تا زیان ناشی از فاجعه‌های طبیعی یا خطاهای امنیتی (که ممکن است در اثر زلزله، طوفان، سیل، آتش‌سوزی، تصادفات، خرابی تأسیسات به‌وجود بیایند) تا حداقل قابل قبولی کاهش یابد. لازم است فرآیندی مدیریت شده برای تعریف و حفظ تداوم فعالیت‌های سازمانی وجود داشته باشد. در این راستا طرح‌های پیوستگی عملیات به‌نحوی نوشته می‌شوند که بتوان براساس آن، ادامه فعالیت‌های سازمانی را تضمین نمود یا بعد از وقفه یا خطا در انجام فعالیت‌ها و در یک دوره زمانی محدود فرآیندهای اصلی سازمان را دوباره به اجرا درآورد و از بروز وقفه دائم در فعالیت‌های سازمان جلوگیری کرد (ایزو/آی ای سی ۲۷۰۰۱: ۲۰۰۵، ۱۳۸۹).

کتابخانه و پیاده‌سازی نظام مدیریت امنیت اطلاعات

کتابخانه‌ها اصولاً منابع حفظ سرمایه‌های فرهنگی، علمی و تاریخی یک ملت هستند که به‌صورت مجموعه‌ای سازمان‌یافته برای دانش‌پژوهان تکامل می‌یابند (تاج‌الدینی و سادات موسوی، ۱۳۸۹). لزوم پرداختن به مسائل امنیتی را در کتابخانه‌ها و مراکز اطلاع‌رسانی نه به‌دلیل ایجاد محدودیت برای کاربران، بلکه کمکی بزرگ به کاربران کتابخانه است. در واقع به این وسیله، امکان مناسب‌تر و بهتری برای کاربران مهیا می‌شود (اوانز، ۱۳۸۷). شاید برای کتابداری لحظه‌ای تلخ‌تر از این پیش نیاید که استفاده‌کننده مشتاقی را به‌سمت کتابی راهنمایی نماید سپس دریابد که کتاب در جای خود نیست و به امانت نیز نرفته است، چه پاسخی باید به مراجعه‌کننده داد: «کتاب ناپدیدشده است؟» (جوکار، ۱۳۸۳).

امروزه با توجه به گرانی کتاب‌ها، تجهیزات و سایر منابع کتابخانه‌ای، امنیت ضرورت بیشتری پیدا کرده است. همیشه شاهد این بوده‌ایم که کتابداران در هنگام بازنشستگی یا تغییر کتابخانه محل خدمت خود با مشکلاتی در خصوص منابع مفقود شده مواجه بوده‌اند که این مسئله باعث شده برخی از کتابداران محدودیت استفاده از منابع کتابخانه‌ای را اعمال نمایند. ضرر این محدودیت‌ها به‌مراتب بیشتر از زیان‌های وارده بر اثر سرقت یا تخریب منابع کتابخانه است. زیرا با اعمال محدودیت هم تصور ناامنی و در نتیجه عدم آرامش شکل می‌گیرد و هم امکان دسترسی به داشته‌های کتابخانه از بسیاری از کاربران سلب می‌شود (نیکنام و فرجی، ۱۳۸۱).

هر ساله کتابخانه‌ها تعدادی از منابع خود را در اثر سرقت از دست می‌دهند و مجبور می‌شوند با صرف بودجه‌ای، نسبت به جایگزینی مجدد آنها اقدام کنند. این مسئله در این وضعیت که بیشتر کتابخانه‌ها

با کمبود بودجه مواجه هستند و بدتر اینکه برخی از منابع از دست‌رفته و به‌علت نایاب و ارزشمند بودن قابل جایگزینی نیستند، اهمیت توجه به مسائل ایمنی را بیشتر می‌کند. (تاج‌الدینی و سادات موسوی، ۱۳۸۹). تأثیر مالی از این دزدی‌ها می‌تواند قابل‌توجه باشد. «برگِل [1]» در یک بررسی دوره‌ای که بر روی موجودی کتابخانه‌اش انجام داد به این نتیجه رسید که ۴ درصد از مجموعه‌اش را به‌علت سرقت از دست داده است، از طرفی تهدید مداوم سرقت در کتابخانه با دارابودن کتاب‌های کم‌یاب همواره وجود دارد (Bregel, 2007).

هدف پژوهش

هدف اصلی از انجام این پژوهش بررسی نظام مدیریت امنیت اطلاعات (امنیت فیزیکی، مدیریت ارتباطات، کنترل دسترسی به اطلاعات و مدیریت حوادث امنیت اطلاعات و مدیریت پیوستگی عملیات) در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران است.

پرسش‌های پژوهش

۱) تا چه میزان امنیت فیزیکی در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران رعایت می‌شود؟

۲) تا چه میزان از امنیت و عملکرد صحیح تجهیزات (نظیر رایانه‌ها) و پردازش اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران اطمینان حاصل می‌شود؟

۳) تا چه میزان جهت دسترسی به اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران کنترل صورت می‌گیرد؟

۴) تا چه میزان در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران در صورت وقوع حادثه در کتابخانه، راهکارهای مدیریتی مرتبط با امنیت کتابخانه رعایت می‌شود؟

۵) تا چه میزان از استمرار در فعالیت‌ها (عدم وقفه در فعالیت‌ها) در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران اطمینان حاصل می‌شود؟

پیشینه پژوهش

در این قسمت مروری بر مرتبط‌ترین و تازه‌ترین پژوهش‌های انجام شده در این حوزه خواهد شد. محمودزاده و رادرجبی (۱۳۸۵) در زمینه مدیریت ارتباطات به بررسی مدیریت امنیت در نظام‌های اطلاعاتی پرداختند. پژوهش با روش سرشماری انجام گرفته است و جامعه آماری این پژوهش شامل

1. Bregel

کاربران رایانه اعم از مدیران و کارمندان سازمان می‌باشند. نتایج نشان داد که مؤلفه عدم آگاهی کاربران بالاترین تهدید برای امنیت اطلاعات نظام‌های رایانه‌ای است. همچنین غفوری (۱۳۸۶) به بررسی آسیب‌شناسی استقرار نظام مدیریت امنیت اطلاعات در سازمان تأمین اجتماعی پرداخت. برای انجام این پژوهش مدیران ارشد و مدیران اجرایی و سایر کاربران می‌باشند که به ترتیب ۳۴ و ۲۴ و ۱۰۵۱ استفاده شد که از این تعداد ۱۶۶ نفر با نمونه‌گیری انتخاب شدند. نتایج نشان داد که ضعف در به‌کارگیری فناوری و محصولات امنیتی از موانع مهم برای استقرار نظام مدیریت امنیت اطلاعات در سازمان تأمین اجتماعی است. اسماعیل‌پور (۱۳۸۸) به بررسی شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات پرداخت. برای انجام این پژوهش، روش تحقیق همبستگی و تحلیل ماتریس همبستگی و به‌طور خاص روش تحلیل عاملی به شناسایی شاخص‌ها و عوامل کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات پرداخته شده است، انجام گرفته است و جامعه آماری این پژوهش متشکل از چند سازمان خصوصی و دولتی نظیر بیمه مرکزی ایران، بیمه پارسیان، بانک صنعت و معدن، رایان سایپا، گروه صنعتی ایران‌خودرو است که در زمینه امنیت اطلاعات در ایران فعالیت اجرایی انجام داده‌اند. نتایج نشان داد که عوامل مربوط به حوزه فنی بر بهبود نظام مدیریت امنیت اطلاعات تأثیر دارند. که در اولویت اول عامل نظامهای حفاظتی و در اولویت بعدی به‌روزرسانی نظام‌ها قرار دارد.

اسماعیل‌پور (۱۳۸۸) در زمینه امنیت فیزیکی به بررسی شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات پرداخت. برای انجام این پژوهش، روش تحقیق همبستگی و تحلیل ماتریس همبستگی و به‌طور خاص روش تحلیل عاملی به شناسایی شاخص‌ها و عوامل کلیدی مؤثر بر بهبود نظام مدیریت امنیت اطلاعات پرداخته شده است، انجام گرفته است و جامعه آماری این پژوهش متشکل از چند سازمان خصوصی و دولتی نظیر بیمه مرکزی ایران، بیمه پارسیان، بانک صنعت و معدن، رایان سایپا، گروه صنعتی ایران‌خودرو است که در زمینه امنیت اطلاعات در ایران فعالیت اجرایی انجام داده‌اند. نتایج نشان داد که عوامل مربوط به حوزه فیزیکی بر بهبود نظام مدیریت امنیت اطلاعات تأثیر دارند؛ که به ترتیب عامل کنترل فیزیکی، مدیریت تجهیزات پشتیبان، مدیریت مرکز داده و مدیریت کارکنان در اولویت قرار دارند. همچنین محبوب، محمدخانی، عابدی (۱۳۸۸) به بررسی ایمنی و امنیت در کتابخانه‌های عمومی استان اصفهان پرداختند. برای انجام این پژوهش، روش پیمایشی انجام گرفته است و جامعه آماری این پژوهش کتابخانه‌های عمومی استان اصفهان می‌باشند. نتایج نشان داد که در بین مقوله‌های مختلف امنیت فضای بیرونی، کنترل ورودی و فضای داخلی دارای وضعیت خوبی هستند و

روشنایی کتابخانه در وضعیت متوسط قرار دارند و همچنین بیات بداقی و فرخی (۱۳۸۹) به بررسی امنیت و ایمنی فیزیکی در کتابخانه‌های عمومی و دانشگاهی استان زنجان پرداختند. روش پژوهش، پیمایشی توصیفی و جامعه آماری این پژوهش ۱۴ کتابخانه و مرکز اطلاع‌رسانی عمومی و دانشگاهی شهر زنجان است. نتایج نشان داد که وضعیت موجود ایمنی فضای کتابخانه‌ها متوسط به‌نظر می‌رسد و با وضعیت مطلوب انطباق صد در صد نداشته است.

هونگ و دیگران[۱] (۲۰۰۳) در زمینه مدیریت پیوستگی عملیات به بررسی نظریه نظام یکپارچه از مدیریت امنیت اطلاعات پرداختند. نشان داد که برای درک مدیریت امنیت اطلاعات، برنامه‌ریزی مدیریت امنیت اطلاعات و پیش‌بینی نتایج مدیریت؛ نظریه نظام یکپارچه مفید است.

میتروپولس، پاتسس و دلاگریس[۲] (۲۰۰۷) در زمینه مدیریت حوادث امنیت اطلاعات به بررسی الزامات پاسخ به حوادث برای نظام مدیریت امنیت اطلاعات تولید شده پرداختند. نتایج نشان داد که در حال حاضر نظام‌ها فاقد توانایی تولید و پاسخ‌گویی به خط‌مشی می‌باشند که عمدتاً به‌دلیل پاسخ‌گویی محدود به حوادث است. همچنین محبوب، محمدخانی، عابدی (۱۳۸۸) به بررسی ایمنی و امنیت در کتابخانه‌های عمومی استان اصفهان پرداختند. برای انجام این پژوهش، روش پیمایشی انجام گرفته است و جامعه آماری این پژوهش کتابخانه‌های عمومی استان اصفهان می‌باشند. نتایج نشان داد که ایمنی در مقابل آتش‌سوزی در وضعیت ضعیف قرار دارد.

ما، جانستون و پیرسون[۳] (۲۰۰۸) در زمینه کنترل دسترسی به بررسی اهداف و فعالیت‌های امنیت اطلاعات پرداختند. برای انجام این پژوهش ۳۵۴ نفر از متخصصان اطلاع‌رسانی امنیت به روش تجربی انتخاب شدند. نتایج در بررسی ۲ سازمان متوسط و کوچک و سازمان بزرگ نشان داد که کنترل دسترسی به‌عنوان مهم‌ترین عامل در فعالیت‌های امنیت اطلاعات شناخته شده است.

روش‌شناسی پژوهش

روش پژوهش با توجه به ماهیت موضوع و اهداف پژوهش، پیمایشی تحلیلی انجام شد. جامعه آماری پژوهش شامل کلیه مدیران کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران (۲۵ مدیر در سال ۱۳۹۱) بودند. لذا تعداد ۲۵ پرسشنامه مورد تجزیه‌وتحلیل قرار گرفت. در پژوهش حاضر از پرسشنامه

1. Hong & et al.
2. Mitropoulos, Patsos & Douligeris
3. Ma, Johnston & Pearson

محقق ساخته بهره گرفته شده است. این پرسشنامه شامل ۱۸ سؤال است که در مقیاس لیکرت ۵ درجه‌ای از ۱ (بسیار کم) تا ۵ (بسیار زیاد) می‌باشد.

به‌منظور گردآوری اطلاعات از چند روش جهت جمع‌آوری پرسشنامه بهره‌گرفته شد که عبارتند از: مراجعه حضوری، ارسال از طریق پست الکترونیکی[1]، از طریق تلفن. هر سه طریق ذکر شده به‌مدت ۲ هفته به‌طول انجامید.

کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران عبارتند از: تهران، علم و صنعت، علامه طباطبایی، امیرکبیر، پیام‌نور، هنر، شهید بهشتی، صنعتی شریف، خواجه نصیرالدین طوسی، علمی کاربردی، علوم اقتصادی، علوم انتظامی، عالی دفاع ملی، صنعت آب و برق شهید عباسپور، تربیت دبیر شهید رجایی، علوم بهزیستی و توانبخشی، علوم پزشکی شهید بهشتی، علوم پزشکی تهران، علوم پزشکی بقیه‌الله، علوم پزشکی ارتش، تربیت مدرس، امام صادق، امام حسین، شاهد و الزهرا.

جهت تجزیه‌وتحلیل داده‌ها از آمار توصیفی همچون فراوانی و درصد جهت بررسی استفاده می‌شود. همچنین از آمار استنباطی نظیر آزمون T تک متغیری جهت بررسی میزان رعایت مؤلفه‌های مدیریت امنیت اطلاعات و نمره کل آن بهره‌گرفته خواهد شد. علاوه بر آن نتایج آزمون مجذورکا یا خی به‌منظور سنجش معناداری تفاوت مابین پاسخ مدیران مورد مطالعه به گزینه‌های سؤالات گزارش داده می‌شود. در نهایت جهت مقایسه مؤلفه‌های مدیریت امنیت اطلاعات از نظر میزان رعایت آنها در کتابخانه‌های مورد مطالعه نتایج آزمون فریدمن ارائه می‌شود.

جهت بررسی پرسشنامه مذکور با استفاده از روایی محتوا[2] پس از تهیه سؤالات پرسش‌نامه از منابع زیر:

۱) پرسشنامه پاکدامن (۱۳۸۸)
۲) پرسشنامه شایان (۱۳۸۷)
۳) و از کتاب استاندارد ISO/IEC 27001: 2005 استفاده گردید.

پرسشنامه پژوهش به اساتید متخصص در رشته علم اطلاعات و دانش‌شناسی داده شد و از آنان خواسته شد تا با عنایت به میزان تناسب هر سؤال با موضوع و اهداف پژوهش نظرات خود را بیان دارند. پس از گردآوری نظرات، تغییراتی در پرسشنامه داده شد تا اینکه پرسشنامه مورد تأیید قرار گرفت و به مرحله اجرا گذاشته شد.

1. Email
2. Content validity

به‌منظور سنجش پایایی پرسشنامه حاضر از ضریب آلفای کرونباخ[1] استفاده گردید که ضریب آن برای ۱۸ ماده و ۲۵ مدیر کتابخانه‌های دانشگاه‌های دولتی مورد مطالعه برابر با ۰/۹۴ به‌دست آمد که ضریب بالایی محسوب می‌شود.

یافته‌های پژوهش

پرسش اول: تا چه میزان امنیت فیزیکی در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران رعایت می‌شود؟

جدول ۱. داده‌های توصیفی و نتایج آزمون مجذورکا براساس تفاوت پاسخ مدیران مورد مطالعه در زمینه میزان رعایت امنیت فیزیکی در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد بررسی

ویژگی‌های آماری / گزینه‌ها	فراوانی	درصد فراوانی	درصد تراکمی	فراوانی مورد انتظار	X^2	درجه آزادی	سطح معناداری
کم	۳	۱۲	۱۲	۶/۳	۱۳/۲۴	۳	۰/۰۰۴
متوسط	۳	۱۲	۲۴	۶/۳			
زیاد	۱۴	۵۶	۸۰	۶/۳			
بسیارزیاد	۵	۲۰	۱۰۰	۶/۳			
جمع کل	۲۵	۱۰۰					

یافته‌ها بیانگر آن است که بیش از نیمی از مدیران کتابخانه‌های مورد مطالعه یعنی ۵۶ درصد (۱۴ نفر) عنوان نموده بودند که امنیت فیزیکی در کتابخانه‌هایشان تا حد زیادی رعایت می‌شود. علاوه بر آن ۲۰ درصد (۵ نفر) مدیران بر این باور بوده‌اند که امنیت فیزیکی در کتابخانه‌هایشان تا حد بسیار زیادی رعایت می‌شود. این در حالی است که ۱۲ درصد (۳ نفر) مدیران اظهار نموده بودند که امنیت فیزیکی در کتابخانه‌هایشان به میزان متوسطی رعایت می‌گردد و به‌همین میزان از مدیران نیز گزارش داده بودند که در کتابخانه‌هایشان به میزان اندکی امنیت فیزیکی رعایت می‌شود. در مجموع نتایج آزمون مجذورکای حاصله در این زمینه دال بر آن بود که مقدار مجذورکای محاسبه شده (x^2= ۱۳/۲۴) از مقدار مجذورکای جدول (x^2= ۱۱/۳۴) با درجه آزادی ۳ در سطح خطای کم‌تر از ۰/۰۱ بزرگ‌تر می‌باشد. بنابراین می‌توان گزارش داد که مابین فراوانی‌های مشاهده شده و مورد انتظار پاسخ مدیران به این سؤال تفاوت معناداری وجود داشته و مدیران کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه اعتقاد داشته‌اند که تا حد زیادی

1. Cronbach`s coefficient alpha

امنیت فیزیکی در کتابخانه‌هایشان رعایت می‌شود.

پرسش دوم: تا چه میزان از امنیت و عملکرد صحیح تجهیزات (نظیر رایانه‌ها) و پردازش اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران اطمینان حاصل می‌شود؟

جدول ۲. نتایج آزمون t تک متغیری جهت بررسی میزان رعایت مدیریت امنیت ارتباطات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

متغیر / ویژگی‌های آماری	میانگین	انحراف معیار	تعداد	میانگین فرضی	تفاضل میانگین‌ها	t	درجه آزادی	احتمال خطا
مدیریت امنیت ارتباطات	۱۸/۷۶	۲/۵۲	۲۵	۱۵	۳/۷۶	۷/۴۶	۲۴	۰/۰۰۰

با توجه به اینکه مؤلفه مدیریت امنیت ارتباطات در پرسشنامه پژوهش حاوی ۵ سؤال در مقیاس لیکرت پنج درجه‌ای از ۱ الی ۵ می‌باشد، لذا دامنه نمرات این مؤلفه بین ۵ الی ۲۵ با میانگین فرضی ۱۵ بوده است. از نتایج به‌دست آمده در این زمینه چنین برمی‌آید که میانگین کسب شده از میزان رعایت امنیت ارتباطات ($\bar{x}$ =۱۸/۷۶) در حدود ۳/۷۶ واحد بیشتر از میانگین فرضی ($\bar{x}$ =۱۵) بوده است. همچنین نتایج آزمون t تک متغیری نیز نشان داد که بین میانگین‌های مشاهده شده و فرضی تفاوت معناداری در سطح خطای کم‌تر از ۰/۰۱ وجود دارد (t_{24} = ۷/۴۶ و P <۰/۰۱). با توجه به این امر می‌توان گفت که در جدول ۲، کتابخانه‌های مورد مطالعه میزان رعایت مدیریت امنیت ارتباطات به‌صورت معناداری بالاتر از حد متوسط بوده و از دیدگاه مدیران کتابخانه‌های مورد بررسی تا حد زیادی از امنیت و عملکرد صحیح تجهیزات و همچنین پردازش اطلاعات در کتابخانه‌هایشان اطمینان حاصل شده است.

پرسش سوم: تا چه میزان جهت دسترسی به اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران کنترل صورت می‌گیرد؟

جدول ۳. نتایج آزمون t تک متغیری جهت بررسی میزان رعایت کنترل دسترسی به اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

متغیر / ویژگی‌های آماری	میانگین	انحراف معیار	تعداد	میانگین فرضی	تفاضل میانگین‌ها	t	درجه آزادی	احتمال خطا
کنترل دسترسی به اطلاعات	۲۳/۹۶	۳/۷۶	۲۵	۱۸	۵/۹۶	۷/۹۳	۲۴	۰/۰۰۰

به جهت آنکه مؤلفه میزان رعایت کنترل دسترسی به اطلاعات در پرسشنامه به‌کار رفته در پژوهش از ۶ سؤال در مقیاس لیکرت پنج درجه‌ای از ۱ الی ۵ تشکیل گردیده، بنابراین دامنه نمرات آن مابین ۶ الی ۳۰ با میانگین فرضی ۱۸ می‌باشد. همان‌طور که مشاهده می‌شود میانگین حاصله از میزان رعایت کنترل

دسترسی به اطلاعات ($\bar{x}$ =۲۳/۹۶) به‌صورت بارزی در حدود ۵/۹۶ واحد بیشتر از میانگین فرضی ($\bar{x}$ =۱۸) بوده است. این در حالی است که نتایج آزمون t تک متغیری در این زمینه نیز بیانگر آن بود که مابین دو میانگین ذکر شده در سطح خطای کم‌تر از ۰/۰۱ تفاوت معناداری وجود دارد (t_{24} = ۷/۹۳ و P >۰/۰۱). همان‌گونه که در جدول ۳ مشاهده می‌شود در کتابخانه‌های مورد مطالعه میزان رعایت کنترل دسترسی به اطلاعات به‌صورت معناداری بالاتر از حد متوسط بوده و به‌عبارت دیگر مدیران مورد مطالعه بر این باور بوده‌اند که در کتابخانه‌هایشان جهت دسترسی به اطلاعات تا حد زیادی کنترل صورت می‌گیرد.

پرسش چهارم: تا چه میزان در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران در صورت وقوع حادثه در کتابخانه، راهکارهای مدیریتی مرتبط با امنیت کتابخانه رعایت می‌شود؟

جدول ۴. نتایج آزمون t تک متغیری جهت بررسی میزان رعایت مدیریت حوادث امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

ویژگی‌های آماری / متغیر	میانگین	انحراف معیار	تعداد	میانگین فرضی	تفاضل میانگین‌ها	t	درجه آزادی	احتمال خطا
مدیریت حوادث امنیت اطلاعات	۶/۴	۱/۵	۲۵	۶	۰/۴	۱/۳۳	۲۴	۰/۱۹۵

به جهت آنکه مؤلفه میزان رعایت مدیریت حوادث امنیت اطلاعات در پرسشنامه پژوهش شامل ۲ سؤال در مقیاس لیکرت پنج درجه‌ای از ۱ الی ۵ بوده است، لذا دامنه نمرات این مؤلفه بین ۲ الی ۱۰ با میانگین فرضی ۶ می‌باشد. همان‌گونه که مشاهده می‌شود میانگین حاصله از میزان رعایت مدیریت حوادث امنیت اطلاعات ($\bar{x}$ =۶/۴) نسبت به میانگین فرضی ($\bar{x}$ =۶) در حدود ۰/۴ واحد بیشتر بوده که بسیار اندک می‌باشد. علاوه بر آن نتایج آزمون t تک متغیری در این مورد نیز نشان‌دهنده آن بود که بین میانگین‌ها هیچ‌گونه تفاوت معناداری در سطح خطای کم‌تر از ۰/۰۵ وجود ندارد (t_{24} = ۱/۳۳ و P >۰/۱۹۵). همان‌گونه که در جدول ۴ مشاهده می‌شود مابین مدیران کتابخانه‌های مورد بررسی از لحاظ میزان رعایت مدیریت حوادث امنیت اطلاعات تفاوت معناداری وجود نداشته و از دیدگاه آنان در صورت وقوع حادثه در کتابخانه‌شان تا حد متوسطی راهکارهای مدیریتی مرتبط با امنیت کتابخانه رعایت می‌شود.

پرسش پنجم: تا چه میزان از استمرار در فعالیت‌ها (عدم وقفه در فعالیت‌ها) در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران اطمینان حاصل می‌شود؟

جدول ۵. نتایج آزمون t تک متغیری جهت بررسی میزان رعایت مدیریت پیوستگی عملیات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

ویژگی‌های آماری / متغیر	میانگین	انحراف معیار	تعداد	میانگین فرضی	تفاضل میانگین‌ها	t	درجه آزادی	احتمال خطا
مدیریت پیوستگی عملیات	۱۱/۰۸	۲/۱۲	۲۵	۹	۲/۰۸	۴/۹۱	۲۴	۰/۰۰۰

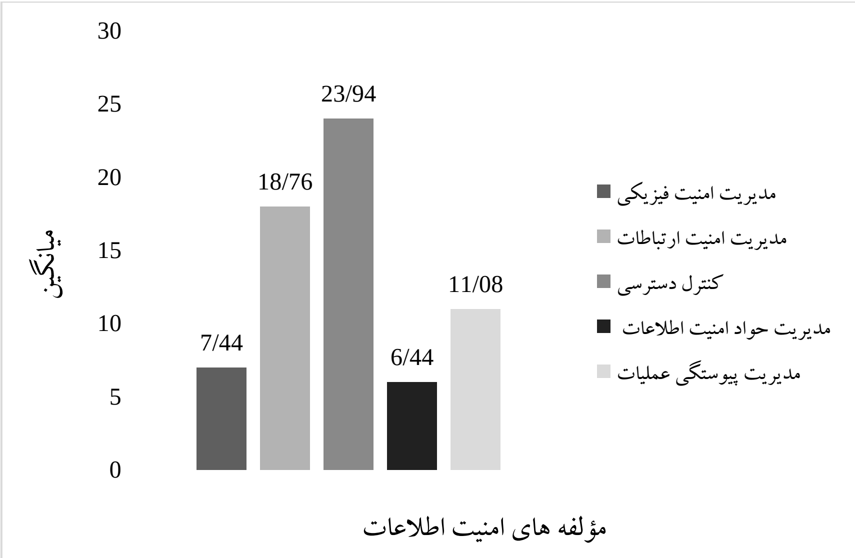
به‌دلیل آنکه مؤلفه میزان رعایت مدیریت پیوستگی عملیات در پرسشنامه به‌کار رفته در پژوهش از ۳ سؤال در مقیاس لیکرت پنج درجه‌ای از ۱ الی ۵ به‌وجود آمده، بنابراین دامنه نمرات آن بین ۳ الی ۱۵ با میانگین فرضی ۹ می‌باشد. یافته‌های حاصله مؤید آن بودند که میانگین به‌دست آمده ($\bar{x}$ =۱۱/۰۸) در حدود ۲/۰۸ واحد از میانگین فرضی ($\bar{x}$ =۹) بیشتر بوده است. همچنین نتایج آزمون t تک متغیری نشان داد که مابین میانگین‌های مشاهده شده و فرضی در سطح خطای کم‌تر از ۰/۰۱ تفاوت معناداری وجود دارد (t_{24} = ۴/۹۱ و P <۰/۰۱). همان‌گونه که در جدول ۵ مشاهده می‌شود میزان رعایت مدیریت پیوستگی عملیات در کتابخانه‌های مورد مطالعه به‌صورت معناداری بالاتر از حد متوسط بوده و به‌عبارت دیگر مدیران کتابخانه‌های مورد مطالعه بر این باور بوده‌اند که در کتابخانه‌هایشان تا حد زیادی مدیریت استمرار در فعالیت‌ها رعایت می‌شود.

جدول ۶. داده‌های توصیفی مؤلفه‌های مدیریت امنیت اطلاعات در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

ویژگی‌های آماری / مؤلفه‌های مدیریت امنیت اطلاعات	میانگین	انحراف معیار	کم‌ترین نمره	بیشترین نمره	تعداد
مدیریت امنیت فیزیکی	۷/۴۴	۱/۴۷	۴	۱۰	۲۵
مدیریت امنیت ارتباطات	۱۸/۷۶	۲/۵۲	۱۵	۲۴	۲۵
کنترل دسترسی به اطلاعات	۲۳/۹۶	۳/۷۶	۱۶	۳۰	۲۵
مدیریت حوادث امنیت اطلاعات	۶/۴	۱/۵	۴	۱۰	۲۵
مدیریت پیوستگی عملیات	۱۱/۰۸	۲/۱۲	۷	۱۴	۲۵

نتایج به‌دست آمده حاکی از آن است که میانگین مؤلفه میزان رعایت کنترل دسترسی به اطلاعات ($\bar{\mathbf{x}}$ =۲۳/۹۶) در مقایسه با سایر مؤلفه‌های مدیریت امنیت اطلاعات بالاتر بوده و پس از آن در درجه دوم میانگین مؤلفه مدیریت امنیت ارتباطات ($\bar{\mathbf{x}}$ =۱۸/۷۶) قرار داشته است. این در حالی است که میانگین مؤلفه مدیریت پیوستگی عملیات ($\bar{\mathbf{x}}$ =۱۱/۰۸) در رتبه سوم قرار داشته و پس از آن میانگین مؤلفه مدیریت امنیت فیزیکی ($\bar{\mathbf{x}}$ =۷/۴۴) بوده است و سرانجام کم‌ترین میانگین در میان مؤلفه‌های مدیریت امنیت اطلاعات

مربوط به مؤلفه مدیریت حوادث امنیت اطلاعات ($\bar{x}$ =۶/۴) بوده است.



نمودار ۱. داده‌های توصیفی مؤلفه‌های مدیریت امنیت اطلاعات
در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

به‌منظور سنجش معناداری تفاوت مابین مؤلفه‌های مدیریت امنیت اطلاعات در زمینه میزان رعایت آنان در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه از آزمون فریدمن بهره گرفته شده که نتایج کسب شده از آن در جدول ۷ آورده شده است.

جدول ۷. نتایج آزمون فریدمن جهت مقایسه مؤلفه‌های مدیریت امنیت اطلاعات
در زمینه میزان رعایت آنان در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد مطالعه

ویژگی‌های آماری / مؤلفه‌های مدیریت امنیت اطلاعات	میانگین رتبه‌ها	تعداد	X^2	درجه آزادی	سطح معناداری
مدیرت امنیت فیزیکی	۱/۸	۲۵	۹۶/۷۴	۴	۰/۰۰۰
مدیریت امنیت ارتباطات	۴/۰۲				
کنترل دسترسی به اطلاعات	۴/۹۸				
مدیریت حوادث امنیت اطلاعات	۱/۲۴				
مدیریت پیوستگی عملیات	۲/۹۶				

هم‌چنان که ملاحظه می‌گردد به‌طور کلی میانگین رتبه‌ها بین مؤلفه‌های مدیریت امنیت اطلاعات در زمینه میزان رعایت آنان در کتابخانه‌های مورد مطالعه از یکدیگر متفاوت می‌باشد، به‌گونه‌ای که میانگین رتبه مؤلفه میزان رعایت کنترل دسترسی به اطلاعات ($\bar{x}_j$ =۴/۹۸) در مقایسه با میانگین رتبه سایر

مؤلفه‌های مدیریت امنیت اطلاعات بالاتر بوده است. با توجه به اینکه توزیع آزمون فریدمن با درجه آزادی $d.f = k - 1$ تقریباً با توزیع آزمون مجذورکا با همان درجه آزادی یکسان می‌باشد، بنابراین نتایج حاصله از آزمون فریدمن را با مقدار مجذورکای جدول مقایسه می‌نماییم. از آنجا که مقدار آزمون فریدمن محاسبه شده در این زمینه (x_{r^2} =۹۶/۷۴) از مقدار مجذورکای جدول (x^2= ۱۳/۲۸) با درجه آزادی ۴ در سطح خطای کم‌تر از ۰/۰۱ بیشتر بوده است، لذا می‌توان نتیجه گرفت بین مؤلفه‌های مدیریت امنیت اطلاعات از لحاظ میزان رعایت آنها در کتابخانه‌های مورد مطالعه تفاوت معناداری با یکدیگر وجود داشته است. با مشاهده داده‌های توصیفی جدول ۶ درمی‌یابیم که در کل میانگین مؤلفه میزان رعایت کنترل دسترسی به اطلاعات ($\bar{x}$= ۲۳/۹۶) نسبت به دیگر مؤلفه‌های مدیریت امنیت اطلاعات بیشتر بوده، بنابراین می‌توان گزارش داد که در کتابخانه‌های مرکزی دانشگاه‌های دولتی مورد بررسی مؤلفه کنترل دسترسی به اطلاعات بیش از سایر مؤلفه‌های مدیریت امنیت اطلاعات رعایت می‌شود.

نتیجه

هدف اصلی از انجام این پژوهش بررسی ۵ مؤلفه این استاندارد: امنیت فیزیکی و ارتباطات، کنترل دسترسی به اطلاعات و مدیریت حوادث امنیت اطلاعات و مدیریت پیوستگی عملیات در کتابخانه‌های مرکزی دانشگاه‌های دولتی شهر تهران بوده است.

یافته‌ها نشان می‌دهد امنیت فیزیکی در کتابخانه‌های مرکزی تا حد زیادی رعایت می‌شود. چنانچه در کتابخانه‌های مرکزی از نظامهای امنیتی پیشرفته و به‌روز نظیر درگاه‌های حفاظتی، دوربین مداربسته، سیستم و ... لحاظ گردد می‌توان امیدوار بود که امنیت فیزیکی در کتابخانه‌ها تأمین شود. نتایج بررسی‌های انجام شده نشان می‌دهد که نتایج پژوهش اسماعیل‌پور (۱۳۸۸) و محبوب، محمدخانی، عابدی (۱۳۸۸) و بیات بداقی و فرخی (۱۳۸۹) با نتایج به‌دست آمده از پژوهش حاضر مطابقت دارد.

همچنین یافته‌ها نشان می‌دهد تا حد زیادی از امنیت و عملکرد صحیح تجهیزات و همچنین پردازش اطلاعات در کتابخانه‌های مرکزی اطمینان حاصل شده است. لذا چنانچه در کتابخانه‌های مورد بررسی نظامهای امنیتی تحت وب باشند و به‌لحاظ امنیتی نسخه پشتیبان از آنها تهیه شود و روزآمد شوند، هم‌چنین در صورت وجود نقص در نظامهای امنیتی به‌سرعت در رفع مشکل آنها اقدام نمایند می‌توان امیدوار بود که امنیت ارتباطات به‌خوبی در کتابخانه‌ها رعایت شود. نتایج بررسی‌های انجام شده نشان می‌دهد که نتایج پژوهش محمودزاده و رادرجبی (۱۳۸۵) و غفوری (۱۳۸۶) با نتایج به‌دست آمده از پژوهش حاضر مطابقت نداشته، این در حالی است که نتایج پژوهش اسماعیل‌پور (۱۳۸۸) با نتایج به‌دست

آمده از پژوهش حاضر مطابقت دارد.

همچنین یافته‌ها نشان می‌دهد تا حد زیادی کنترل دسترسی به اطلاعات در کتابخانه‌های مرکزی رعایت می‌شود. نتایج فرضیه نیز نشان می‌دهد که این مؤلفه نسبت به سایر مؤلفه‌های امنیت اطلاعات در کتابخانه‌ها رعایت می‌شود. بنابراین لازم است در کتابخانه‌ها سطح دسترسی کاربران، کارمندان و مدیران تعریف شود و یک شناسه کاربری و رمز عبور برای افراد اختصاص یابد و در صورت دسترسی افراد غیرمجاز به منابع اطلاعاتی کتابخانه موارد انضباطی به‌کار گرفته شود. در این صورت می‌توان امیدوار بود که از دسترسی به اطلاعات برای افراد تعریف نشده اطمینان حاصل شده است. نتایج بررسی‌های انجام شده نشان می‌دهد که نتایج پژوهش جانستون و پیرسون (۲۰۰۸) با نتایج به‌دست آمده از پژوهش حاضر مطابقت دارد. نتایج فرضیه نیز نشان می‌دهد که میانگین مؤلفه میزان رعایت کنترل دسترسی به اطلاعات در مقایسه با سایر مؤلفه‌های مدیریت امنیت اطلاعات بالاتر بوده است، در نتیجه مؤلفه کنترل دسترسی به اطلاعات بیش از سایر مؤلفه‌های مدیریت امنیت اطلاعات رعایت می‌شود.

علاوه بر این یافته‌ها نشان می‌دهد در صورت وقوع حادثه در کتابخانه‌های مرکزی راهکارهای مدیریتی مرتبط با امنیت کتابخانه رعایت می‌شود و از طرفی نتایج آزمون t تک متغیری نیز نشان داد بین مدیران کتابخانه‌های مورد بررسی از لحاظ میزان رعایت مدیریت حوادث امنیت اطلاعات تفاوت معناداری وجود نداشته و از دیدگاه آنان در صورت وقوع حادثه در کتابخانه‌شان تا حد متوسطی راهکارهای مدیریتی مرتبط با امنیت کتابخانه رعایت می‌شود. بنابراین لازم است موارد امنیتی جهت جلوگیری از آتش‌سوزی، ترکیدگی لوله، قطعی برق، زلزله، سیل و ... لحاظ گردد تا در صورت وقوع این حوادث، منابع اطلاعاتی کتابخانه کم‌تر در معرض نابودی قرار بگیرند. در این صورت است که می‌توان امیدوار بود مدیریت حوادث امنیت اطلاعات در کتابخانه‌ها رعایت شده است. نتایج بررسی‌های انجام شده نشان می‌دهد که نتایج پژوهش میتروپولس، پاتسس، دلاگریس (۲۰۰۷)، محبوب، محمدخانی و عابدی (۱۳۸۸) با نتایج به‌دست آمده از پژوهش حاضر مطابقت ندارد.

در نهایت یافته‌ها نشان می‌دهد تا حد زیادی مدیریت استمرار در فعالیت‌ها در کتابخانه‌های مرکزی رعایت می‌شود. لازم است در کتابخانه‌ها فرآیندهای کتابخانه‌ای در فواصل منظم و نامنظم مورد بررسی قرار گیرند تا در صورت رخ دادن مشکلات امنیتی از به‌وجود آمدن وقفه در فعالیت‌های کتابخانه‌ای جلوگیری به عمل آید. نتایج بررسی‌های انجام شده نشان می‌دهد که نتایج پژوهش هونگ (۲۰۰۳) با نتایج به‌دست آمده از پژوهش حاضر مطابقت ندارد.

پیشنهادهای پژوهش

لازم است جهت امنیت فیزیکی در کتابخانه‌ها، در ایستگاه‌های مخصوص، وسایل شخصی افراد تحویل گرفته شود، درگاه‌های حفاظتی، دوربین مداربسته و ... لحاظ گردد، سپس به کاربران اجازه دسترسی به منابع کتابخانه‌ای داده شود. با این راه‌حل می‌توان از به سرقت رفتن و صدمه رساندن منابع کتابخانه‌ای اطمینان حاصل نمود. لازم است جهت امنیت ارتباطات از نظام‌های اطلاعاتی‌ای در کتابخانه‌ها استفاده شود که: به‌روز باشند، به لحاظ امنیتی پشتیبانی شوند، بتوانند تحت وب باشند، هم‌چنین این امکان وجود داشته باشد بتوان نسخه پشتیبان از اطلاعات تهیه نمود و در نهایت در صورت وجود نقص در نظام‌های امنیتی به‌سرعت در رفع مشکل آنها اقدام نمایند، پیشنهاد می‌شود جهت امنیت کنترل دسترسی به اطلاعات در کتابخانه برای مدیران، کارمندان و کاربران شناسه کاربری و رمز عبور در نظر بگیرد و سطوح دسترسی افراد به منابع کتابخانه‌ای را مشخص نمایند. به‌عبارت دیگر سطح دسترسی یک مدیر گسترده‌تر از سطح دسترسی کارمندان است و سطح دسترسی کارمندان گسترده‌تر از سطح دسترسی کاربران است و در صورت دسترسی افراد غیرمجاز به منابع اطلاعاتی کتابخانه موارد انضباطی به‌کار گرفته شود. بایستی جهت جلوگیری از حوادث در کتابخانه‌ها لوله‌های آب فرسوده تعویض شوند، برق اضطراری به هنگام قطع برق برای مدت طولانی به‌کار گرفته شود. به‌عبارت دیگر موارد امنیتی جهت جلوگیری از آتش‌سوزی، ترکیدگی لوله، قطعی برق، زلزله، سیل و ... لحاظ گردد. تا اگر این حوادث رخ دهد، منابع اطلاعاتی کتابخانه کم‌تر در معرض نابودی قرار بگیرند. در نهایت جهت مدیریت پیوستگی عملیات بهتر است در صورتی‌که کارمندی به مرخصی برای مدت طولانی می‌رود امکان جایگزینی با کارمندی دیگر در نظر گرفته شود و فرآیندهای کتابخانه‌ای در فواصل منظم و نامنظم مورد بررسی قرار گیرند تا در صورت رخ دادن مشکلات امنیتی از به‌وجود آمدن وقفه در فعالیت‌های کتابخانه‌ای جلوگیری به عمل آید.

پیشنهادهایی برای پژوهش‌های آینده

چنانچه هر یک از مدیران، کارمندان و کاربران کتابخانه‌های مورد مطالعه متناسب با امکانات و شرایط فعلی و در نظر گرفتن شرایط آینده موارد امنیتی را رعایت نمایند، به‌عبارت دیگر چنانچه دستورالعمل‌های مرتبط با مؤلفه‌های امنیت اطلاعات به طریق صحیح به‌کار گرفته شود می‌توان امیدوار بود امنیت اطلاعات در کتابخانه‌های مورد بررسی به‌طور نسبی رعایت شود.

توصیه می‌شود علاقه‌مندان به این حیطه موضوعی هر مورد از مؤلفه‌های ۱۱ گانه استاندارد را به‌صورت دقیق‌تر و با جزئیات کامل در کتابخانه‌ها بررسی کنند تا بشود با اظهارنظرهای مدیران کتابخانه

تطابق داد و بشود با مقایسه بین این پژوهش و پژوهش‌های آینده نتیجه‌گیری علمی‌تر و عملی‌تر دریافت کرد. این مؤلفه‌ها عبارت‌اند از: خط‌مشی امنیت اطلاعات، سازمان‌دهی امنیت اطلاعات، مدیریت منابع، امنیت نیروی انسانی، امنیت فیزیکی، مدیریت ارتباطات، کنترل دسترسی، مدیریت حوادث امنیت اطلاعات، طرح تداوم کسب و کار، مدیریت پیوستگی عملیات و انطباق با قوانین امنیتی.

کتابنامه

اسدی، مریم (۱۳۸۴). فناوری‌های اطلاعات: با یک دیدگاه طبقه‌بندی. *علوم اطلاع‌رسانی*، ۲۰(۳ و ۴)، ۱-۱۶.

اسماعیل‌پور، حمیدرضا (۱۳۸۸). *شناسایی و رتبه‌بندی عوامل و شاخص‌های کلیدی مؤثر بر بهبود سیستم مدیریت امنیت اطلاعات. پایان‌نامه کارشناسی ارشد*، دانشگاه شهید بهشتی تهران.

امیرخانی، امیرحسین؛ توکلی، جمیله (۱۳۸۸). چالش‌های امنیت اطلاعات در سازمان‌ها. *عصر فناوری اطلاعات*، ۵۱، ۷۵- ۷۸.

اوانز، ادواردجی (۱۳۸۷). *فنون مدیریت برای کتابداران*. مشهد: بنیاد پژوهش‌های اسلامی، آستان قدس رضوی.

بیات بداقی، ناهید؛ فرخی، فرهنگ (۱۳۸۹). امنیت و ایمنی فیزیکی در کتابخانه‌های عمومی و دانشگاهی استان زنجان. *فصلنامه کتاب*، ۸۴ ۲۲-۳۳.

پاکدامن، راضیه (۱۳۸۸). *ارائه چارچوب پیاده‌سازی سیستم مدیریت امنیت اطلاعات (ISMS) در بخش فناوری اطلاعات در سازمان‌ها و ارائه سیستم خبره (مشاور) آن*. پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس تهران.

پورمند، علی (۱۳۸۵). استانداردی برای مدیریت امنیت اطلاعات. *تدبیر*، ۱۷۸، ۵۹-۶۱.

تاج‌الدینی، اورانوس؛ سادات موسوی، علی (۱۳۸۹). مدیریت امنیت در معماری فضاهای کتابخانه‌ای. *کتاب ماه کلیات*، ۱۴۹، ۶۴-۶۷.

جعفری، نیما؛ صادقی مجرد، مرجان (۱۳۸۶). سیستم مدیریت امنیت اطلاعات از طرح تا اصلاح. *تدبیر*، ۱۸۹، ۵۹-۶۲.

جوکار، طاهره (۱۳۸۳). مبانی و اصول مدیریت امنیت در کتابخانه‌ها. *فصلنامه کتاب*، ۵۹، ۵۱-۶۲.

خراسانی‌راد، ایمان؛ حسین‌آبادی، حسن؛ امیرزاده، رامین (مترجمان) (۱۳۸۹). *استاندارد ISO/IEC 27001: 2005*. تهران: توف نورد ایران.

داوری دولت‌آبادی، مجید (۱۳۸۹). *مرجعی بر امنیت، مبتنی بر CompTIA Security*. تهران: پندار پارس: سخنوران: مانلی.

سیفی، مهدی؛ شربت اوغلی، احمد (۱۳۸۶). *ممیزی و مدیریت امنیت اطلاعات: راهکارها و استانداردهای امنیتی*. تهران: انستیتو ایز ایران.

شایان، علی (۱۳۸۷). *طراحی مدل جامع مدیریت امنیت اطلاعات در بانکداری الکترونیکی*. پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس تهران.

غفوری، محمدحسین (۱۳۸۶). *آسیب‌شناسی استقرار سیستم مدیریت امنیت اطلاعات در سازمان تأمین اجتماعی*. پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران شمال تهران.

محبوب، سیامک؛ محمدخانی، آرش؛ عابدی، یوسف (۱۳۸۸). *ایمنی و امنیت در کتابخانه‌های عمومی استان اصفهان. در همایش ملی معماری فضاهای کتابخانه‌ای، اصفهان، آذر ۵ و ۴*. اصفهان: [بی‌نا].

محمودزاده، ابراهیم؛ رادرجبی، مهدی (۱۳۸۵). مدیریت امنیت در سیستم‌های اطلاعاتی. *فصلنامه علوم مدیریت ایران*، ۱ (۴)، ۷۸-۱۱۲.

معتمدی‌فر، مرتضی (۱۳۸۷). *روش پیاده‌سازی استاندارد امنیت اطلاعات (ISO 27001) در ادارات و سازمان‌ها*. تهران: مرکز آموزش و تحقیقات صنعتی ایران.

نیکنام، مهرداد؛ فرجی، ایرج (۱۳۸۱). *دائره‌المعارف کتابداری و اطلاع‌رسانی* (ویرایش ۲). (ج.۱، ص ۷۴۹-۷۵۳). تهران: کتابخانه ملی جمهوری اسلامی ایران.

هاروی، راس (۱۳۸۴). *آسیب‌شناسی مواد کتابخانه: اصول، راهبردها و شیوه کار کتابداران*، ترجمه علی اشکویی، تهران: دبیزش.

Ayre, L. (2003). *Infopeople Project How-To Guides: Library Computer and Network Security*. California: State Librarian. Available at: http://www.galecia.com/included/docs/ayre_library_computer_and_network_security.pdf. Accessed (2012 January 5).

Bregel, L. (2007). "*Create a more human library*". US: 3M Library Systems. Available at: http://multimedia.3m.com/mws/mediawebserver?mwsId=66666UuZjcFSLXTtmxT248TcEVuQEcuZgVs6EVs6E666666. Accessed (2012 January 20).

Chair, P. W., Barczyk, E., Burn, T., Carr, C., Daly, M., Danford, R. (2010). *LIBRARY SECURITY GUIDELINES DOCUMENT*. Available at: http://www.ala.org/llama/sites/ala.org.llama/files/content/publications/LibrarySecyGuide.pdf. Accessed (2012 February 14).

Hong, K.S., Chi, Y.P., Chao, L. R., Tang, J. H. (2003). An integrated system theory of information security Management. *Information Management & Computer Security*, 11(5), 243 – 248. Available at: http://www.emeraldinsight.com/journals.htm?issn=0968-5227&volume=11&issue=5&articleid=862860&show=abstract. Accessed (2012 January 30).

Ma, Q., Johnston, A. C. & Pearson, M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, 16(3), 251 – 270. Available at: http://www.emeraldinsight.com/journals.htm?issn=0968-5227&volume=16&issue=3&articleid=1736848&show=html. Accessed (2012 April 2).

Mitropoulos, S.; Patsos, D. & Douligeris, C. (2007). Incident response requirements for distributed security information management systems. *Information Management & Computer Security*, 15(3), 226- 240. Available at: http://www.emeraldinsight.com/journals.htm?issn=0968-5227&volume=15&issue=3&articleid=1610925&show=abstract. Accessed (2012 January 30).

National Institute of Standard and Technology (NIST) (2006). *Information Security Handbook: A Guide for Managers*. United States of America: NIST. Available at: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf. Accessed (2012 February 22).

Swanson, D. (2006). *IT AUDIT CHECKLIST SERIES: Information Security practical guidance on how to prepare for successful audits*. IT Compliance Institute. Available at: http://www.t2pa.com/library/it-audit-checklists. Accessed (2011 May 8).